The black market of personal data: financial, legal and social aspects

Elena Sergushina[1], *Oleg* Kabanov[1*], *Andrei* Egorov[2], *Vitaliy* Pomazanov[3], *Natalya* Pluzhnikova[4], and *Pavel* Savchenko[5]

[1]Ogarev Mordovia State University, 68, Bolshevitskaya str., 430005, Saransk, Russia
[2]Pskov branch of the Academy of the Federal Penitentiary Service of Russia, 28, Zonal Highway, 180014 Pskov, Russia
[3]I.T. Trubilin Kuban State Agrarian University, 13, st. Kalinina, 350044, Krasnodar, Russia
[4]Moscow Technical University of Communications and Informatics, 8-A, str. Aviamotornaya, 111024, Moscow, Russia
[5]Russian University of Transport (MIIT), 9b9, Obrazcova Ulitsa, 127994 Moscow, Russia

Abstract. This article touches on the topic of the black market of personal data. The concept of the "black market of personal data" and the description of its financial, legal and social aspects are considered. The relevance of this topic lies in the fact that offers on the black market have not only not decreased, on the contrary, their number has visibly increased. This article describes the basic rules for the security of personal data storage. Keywords: black market, personal data, user, messenger, darknet, information, database.

1 Introduction

There is a law on personal data in Russia. In order to collect, process and store data about employees, subscribers to the newsletter and site visitors, you almost always need to get their consent, and store the data in Russia.

Any data, whether personal or not related to a person's personality at all, has value for business if it meets three characteristics at once - relevance, reliability, completeness.

Data with all these properties are very rare on the black market. But even if suddenly a large array of full-fledged data appeared on the darknet (for example, this is a completely fresh database of some reputable personal data operator), no one will ever be able to guarantee their quality. The operator, of course, will be interested in the fastest destruction of the consequences of the leak and will never contact the buyer from the darknet. And it is completely illogical to believe the seller of stolen data.

From January to September 2020, 96.5 million records of personal data and payment information leaked in Russia (according to InfoWatch). At the same time, the share of leaks related to fraudulent actions exceeds 10% — this figure is three times lower in the world (Figure 1).

* Corresponding author: jhostmc@mail.ru

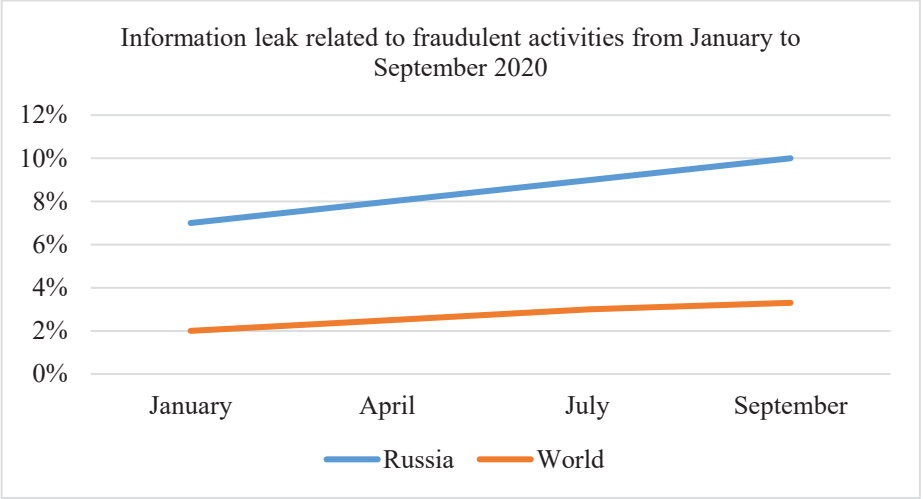

Fig. 1. Information leakage related to fraudulent activities from January to September 2020.

2 The main part

The black market of personal data is constantly growing, and the main reason for this is insiders - employees of companies that sell or give away confidential data of their customers for free, according to a study by the IT company Krok (Forbes has it). In 2020, the total damage from personal data leaks exceeded 3 billion rubles, according to the materials of Krok.

The sale of personal data on the darknet takes place through special forums or marketplaces. The transaction is carried out directly or through a guarantor - a person who verifies that the information provided by the seller corresponds to the buyer's request [1-7].

In the darknet, you can find various personal information - from a simple email address to a complete data package for a specific person.

The stolen information is used to make fake passports and other fake identity cards — the stolen data is superimposed on photos taken in the editor. Sale of the Fullz database ($100 for data about one person) contributes to the development of SIM card fraud, when an attacker using stolen data convinces a mobile operator that he is a real customer who has lost his phone and wants to get a new SIM card. After activating the card, the fraudster gains control of the victim's mobile number and uses it to change passwords and gain access to the bank account.

In addition, the stolen data can be used with the help of free software to try to log in to sites that require only a login and password [5].

Personal data refers to any personal information about a person that could help identify him or find his property or place of residence. The Russian market for the sale of personal data in the shadow sector of the Internet, the so-called dark net'e (access to its sites is only available using Tor or similar software), is not well researched. Much more extensive statistics are collected in the US market, where information is consolidated with the help of specialized agencies. But the American data helps to draw up a picture of what is happening on the Russian market, taking into account the significantly smaller scale of what is happening.

Let's say a company has bought some database on the darknet. Most likely, it is irrelevant and/or unreliable. Why did she do that?

The first goal is to use it as a potential customer base. But "cold" calls from unknown numbers, and even with the wrong commercial offer, can only damage business. An actual example from the world of auto insurance. Many car owners have faced calls from insurance agents who offered "the best conditions" for a car that has been sold for a long time. Naturally, such contacts with a potential client can only cause irritation (and sometimes a complaint to Roskomnadzor, but more on that below). The use of any data, the origin of which you cannot explain to the client, damages the reputation of the company [1-10].

The second purpose of the purchase is that the company wants to know more about the customer. She needs information about whether he travels abroad, whether he has a car, etc. But buying data on the black market will not be able to answer this question. If indirect signs about the well-being and lifestyle of the client are important to the company, then the relevance of the information is important to it. Has he lost his job three months ago, can he travel abroad right now, or even better, has he already bought a plane ticket (for example, to sell insurance)? And this requires not dubious sources, but access to really relevant, and even better, reference databases.

The third goal is the fight against fraud, checking customer information (for example, passport data). Only reference sources really work here. The company needs reliability guarantees, and no one gives them on the darknet.

The processing of personal data means any action with them, including their collection, recording, systematization, accumulation, storage, clarification (updating, modification), extraction, use, transfer (distribution, provision, access), depersonalization, blocking, deletion, destruction.

As a general rule, the processing of personal data and the transfer of this obligation to another person is allowed only with the consent of the data subject. At the same time, consent to data processing must be specific, informed, conscious and can be withdrawn at any time. Without it, operators1 and other persons who have gained access to personal information are not entitled to disclose and distribute data, unless otherwise provided by federal law[11-15].

There are cases when documents containing personal data, including copies of contracts, passports, questionnaires, were thrown into the trash. The reasons for such behavior may be the negligence of employees, the lack of a formed culture of "confidentiality" and employers' control over its compliance, and sometimes proper conditions for storing documentation. An equally significant factor is that now there is no total control over compliance with the requirements by the regulator - Roskomnadzor.

Sometimes information becomes available to outsiders due to carelessness: when data is sent by e-mail via unsecured communication channels (without the use of encryption tools) or via messengers. There are cases of "innocent" data dissemination through selfies. Also, the information is disclosed by copying it to flash cards or as a result of the removal of documents that have not been completely destroyed from the building of the organization.

Sometimes personal information is disclosed by the operator's employees intentionally for selfish reasons. As a result, credit card data, passports, customer profiles may fall into the hands of fraudsters.

The problem of criminal data penetration is relevant today for the whole of Russia, although most often employees of telecom operators, bank managers and civil servants in the regions are engaged in this, Andrey Arsentiev, head of analytics and special projects at InfoWatch Group, told Forbes. This is due to both a lower level of security of information resources and low salaries, Arsentiev argues. His words are confirmed by the data of the GAS "Justice" system: according to information from it, 43 cases under criminal article 138 h were considered in 2020. 2 - violation of the secrecy of correspondence, telephone conversations, postal, telegraphic or other communications of citizens. There are only five such cases so far this year [1,8,13].

In May 2020, a specialist of the Vimpelcom office in Kazan, M.V. Burlak, received a fine of 120,000 rubles for punching and sending his friend data on calls from his ex-wife, it follows from the court materials. The boatman did it for free, and also attracted his colleague, whose name is not disclosed, to the breakdown. The information about the calls was forwarded by the Boatman to the customer via the WhatsApp messenger. When the victim realized that her ex-husband was aware of the details of her communication by mobile phone, she wrote a complaint to Vimpelcom. Later, the operator's security service and the FSB contacted her, according to the case materials. Court cases against the victim's ex-husband and another employee of Vimpelcom, who appeared in the case, are still underway [13-17].

Another similar case occurred in Yakutia, where in June 2020, the seller of the office of one of the mobile operators, Patrangel V.O., was punished with 200 hours of community service for leaking subscriber calls in one month. In July 2019, an Internet user wrote to Patrangel asking him to send a list of outgoing and incoming calls from a certain number for June of the same year. Patrangel entered the call detail viewer of the SSVO, using his service username and password, entered the phone number and received information about the calls. After that, the criminal copied the data to Excel, uploaded it to his mobile phone and sent it to the customer. How much money Patrangel received for such "work" is not indicated in the court documents, the FSB was also engaged in its development. The identity of the customer could not be established.

"Most employees don't think about the fact that their messengers are controlled."

For violation of the rules of personal data processing, a whole range of types of administrative responsibility has been established. At the same time, if several violations are revealed during the audit, they will be held accountable for each of them, including separately for each "episode". Also, both the organization and the guilty individual – an employee of the organization - can be held responsible for the violation at the same time (Part 3 of Article 2.1 of the Administrative Code of the Russian Federation) [1-14].

The main type of administrative punishment for violation of the legislation on personal data is a fine, the amount of which depends on the specific violation. The maximum possible is 75,000 rubles. It is provided for the organization for processing personal data without the written consent of a citizen, when such consent is required, or for the absence of all necessary information in it (Part 2 of Article 13.11 of the Administrative Code of the Russian Federation).

If a leak of non-essential personal data is found, a person faces a fine of up to 50,000 rubles, and a legal entity - up to 6 million rubles, says Alexey Gavrishev, managing partner of AVG Legal law company.

The penalty for violating the secrecy of telephone conversations and correspondence can be up to four years in prison, Gavrishev noted. In addition, the information that passes through the telecom operator is most often a trade secret, and its disclosure is punishable by imprisonment for up to five years

Below are the types of administrative responsibility relevant to the situation of data purchased on the black market (Figure 2).

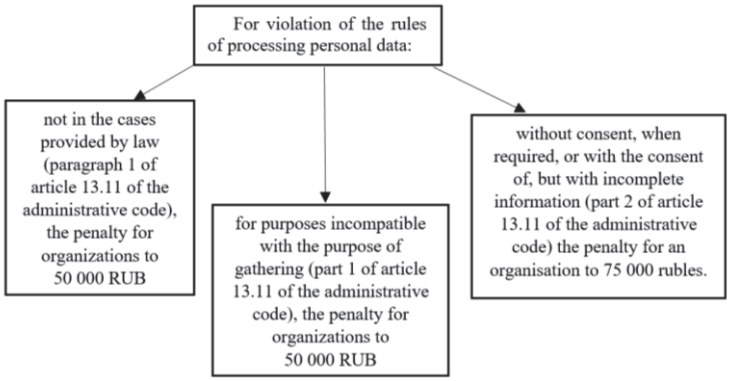

Fig. 2. Administrative penalties for violation of personal data processing rules.

For violation of the rules of processing personal data:

• not in the cases provided by law (paragraph 1 of article 13.11 of the administrative code), the penalty for organizations to 50 000 RUB;

• for purposes incompatible with the purpose of gathering (part 1 of article 13.11 of the administrative code), the penalty for organizations to 50 000 RUB;

• without consent, when required, or with the consent of, but with incomplete information (part 2 of article 13.11 of the administrative code) the penalty for an organisation to 75 000 rubles.

Failure to comply with personal data protection requirements:

• o not publish the necessary documents on your policy in relation to the processing of personal data and on what requirements to protect you sell or otherwise provide unrestricted access to them (part 3 of article 13.11 of the administrative code), the penalty for the organization – 30 000 RUB.;

• o not ensure the safety of data during manual processing, if this entails unlawful or accidental access, destruction, modification, blocking, copying, provision, dissemination or other misconduct (section 6 of article 13.11 of the administrative code), the penalty for the organization - 50 000 RUB.;

Non-fulfillment of obligations when interacting with Roskomnadzor:

* do not provide the information requested by them in accordance with Part 3 of Article 23 of the Law on Personal Data (Article 19.7 of the Administrative Code of the Russian Federation);

* do not comply with the legal order of Roskomnadzor on the elimination of violations on time (Part 1 of Article 19.5 of the Administrative Code of the Russian Federation);

* you will hinder the inspection or evade it (Part 1 of Article 19.4.1 of the Administrative Code of the Russian Federation);

* do not comply with Roskomnadzor's requirement to clarify, block or destroy personal data if they are incomplete, inaccurate, outdated, illegally obtained or are not necessary for processing purposes (Part 5 of Article 13.11 of the Administrative Code of the Russian Federation) [4-9] (Figure 3).

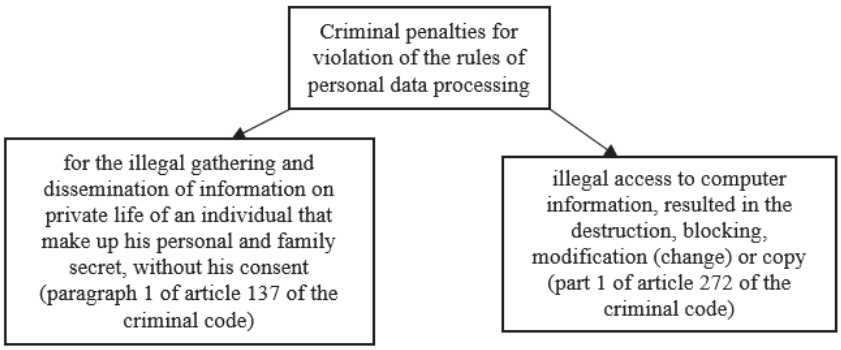

Fig. 3. Criminal penalties for violation of personal data processing rules.

Separately, we will point out the prospect of criminal liability. Although there is no special rule on liability for violation of the legislation on personal data in the Criminal Code of the Russian Federation, the actions of a person who violated the rules for working with personal data may constitute another crime, in particular:

• for the illegal gathering and dissemination of information on private life of an individual that make up his personal and family secret, without his consent (paragraph 1 of article 137 of the criminal code);

• illegal access to computer information, resulted in the destruction, blocking, modification (change) or copy (part 1 of article 272 of the criminal code).

Of course, only an individual can be brought to criminal responsibility (Article 19 of the Criminal Code of the Russian Federation). However, bringing a guilty individual to criminal responsibility does not exempt an organization from administrative responsibility (Part 3 of Article 2.1 of the Administrative Code of the Russian Federation) [8-16].

The sale or transfer of personal data of clients for companies is primarily a reputational loss, says Konstantin Ankilov, CEO of TMT Consulting. But operators also spend money to solve this problem — they have to keep an increased security staff that deals with the problem of leaks, as well as spend money on legal costs when such cases reach court, the expert says. To reduce the number of leaks, it is necessary to rebuild the system of employee access to subscriber data, according to the CEO of Telecom Daily Denis Kuskov. According to him, it is necessary to implement such solutions so that no one can get information about customer calls, for example, without presenting special codes that would show the feasibility of obtaining data. If this is not done, then the mobile penetration market will exist for many more years, complains Kuskov.

Now, to prevent leaks, companies are implementing systems using machine learning to identify the most likely channels of leaks and employees who could potentially become insiders, says Alexander Chernykhov, a leading expert in the information security field of Krok. Digital marking systems for documents and interfaces are being developed to investigate leaks, which also helps in the search for insiders, he noted [7-17].

A representative of Sberbank told Forbes that in 2020, the company did not find a single case of leakage of personal data from bank employees. This was made possible thanks to the "new architecture of processes to counter leaks," noted in the "Savings Bank", but did not disclose the details of working with this problem. MTS has an architectural differentiation of access to information, a full range of technical protection against the dissemination of personal data has also been developed — these are software and technical means of access control and constant monitoring, the representative of the operator said. He added that the company also tells employees that outsiders should not

be allowed to access the protected information, and that criminal liability is threatened for this.

The black market of data has really scaled, including due to the transition of some sellers and buyers to messengers, and this trend will continue due to the general economic crisis, Dmitry Budorin believes:

"Very soon, people who have lost their jobs will go into small-scale hacking. Those forums that sold merged databases have already become known to a wide range of people. The more enterprising began to organize sales channels through messengers in order to earn not on the hacks themselves, but on the resale of information."

It is not entirely correct to talk about the "boom" of leaks that has begun, Knysh believes. In his opinion, recently merged databases have been talked about more often, primarily because there is more information itself.

"It is necessary to protect the data not from leakage, but from unauthorized use," Knysh stressed [1-9].

Today we provide our data to various services and structures, whether it is a loan or a Netflix subscription, because it is quite difficult to talk about the full protection of our privacy.

"We have already passed privacy, we have missed it — we are all in the digital world. Pandora's box is already open," Sergey Solonin, head of the Qiwi payment service, said last year.

Nevertheless, some steps can be taken to secure your data:

* do not link your social media accounts and email to the main phone number that you use as a contact in various services. Get a separate SIM card for these purposes, the number of which will be known only to you. Do not insert this SIM card into your main phone.

* get different mail — working and for personal purposes. Delete emails containing confidential information (passwords, passport details, phone numbers).

* use two-factor identification, but not via SMS. Use services like Google Authenticator.

* set passwords consisting of a large number of characters of different types (numbers, capital and small letters). Do not use the same password for multiple emails.

* periodically check your email for hacking. You can do this using services like Have I Been Pwned or HackenAI.

3 Conclusion

Thus, the following conclusions can be drawn:

Firstly, not only have there been no fewer offers on the black market, on the contrary, their number has visibly increased. Perhaps the number of resellers of the same data has increased, but there is definitely no shortage of offers.

Secondly, prices for almost everything have increased. Especially noticeable is the rise in prices for the so-called bank "breakout". It can be assumed that banks are actively (but some of them have so far unsuccessfully) trying to combat this phenomenon, which causes prices to rise.

Thirdly, judging by the number of offers, low prices and the range of "services", with the security of user data from some mobile operators, everything is very bad. It is in this segment that there is the widest selection of sellers and data (from all kinds of statements to constant tracking of the subscriber's geolocation). "Competition" for these operators can only be made by government agencies – prices are not high here, but there is a rich choice.

In addition, the current level of risk for data providers is affected. Law enforcement officers and security services of banks or telecom operators are fighting against them. And, for example, if a special operation was recently carried out against "breakouts" or mass data drains, then prices are rising.

References

1. *General Data Protection Regulation - General Data Protection Regulation* (2016)
2. *Foreign Account Tax Compliance Act – "The Law on Tax Reporting on Foreign Accounts"* (USA, 2010)
3. *Letter dated 21.09.2018 No. 08-77473, paragraphs 2-11 of Part 1 of Article 6, Part 2 of Article 10 and Part 2 of Article 11 of Federal Law No. 152-FZ of 27.07.2006*
4. *Paragraph 14 of Article 4 of Law No. 223-FZ, Part 4 of Article 4 of Law No. 44-FZ, paragraph 2 of the Rules from Government Decree No. 1084 of 28.11.2013*
5. *Roskomnadzor will check Burger King and Procter & Gamble*, URL: www.rg/2019/01/28/roskomnadzor-proverit-proctergamble-i-burger-king.html?utm_source=yxnews&utm_medium=mobile
6. *"Web scraping" (transl. "content parsing") is a popular method of getting content for free*
7. *The data of 48 million users of social services were found on the Network*, URL: www.infowatch.ru/analytics/leaks_monitoring/20212
8. *Ibid. 9personal values: how Russians will be able to make money on data about themselves*, URL: www.rbc.ru/technology_and_media/19/11/2018/5bf27a9e9a7947bed179806a
9. *Federal Law No. 34 of 18.03.19 "On Amendments to Parts One, Two and Article 1124 of Part Three of the Civil Code of the Russian Federation"*
10. *FRII has developed a draft law on the regulation of personal data*, URL: www.iidf.ru/media/articles/fond/frii-proekt-zakona-o-regulirovanii-personalnykh-dannykh/
11. *Personal values: how Russians will be able to make money on data about themselves*, URL: www.rbc.ru/technology_and_media/19/11/2018/5bf27a9e9a7947bed179806a
12. *Determination of the Moscow City Court in case No. 33-30344*, URL: http://www.mos-gorsud.ru
13. E.S. Sergushina, O.V. Kabanov, A.A. Grigoryev et al, Journal of Critical Reviews **7(3)**, 181-184 (2020) doi:10.31838/jcr.07.03.33
14. E.S. Sergushina, O.V. Kabanov, M.N. Ermakova et al, Opcion **36(27)**, 1377-1385 (2020)
15. S.E. Sergeevna, K.O. Vladimirovich, U.I. Igorevna et al, Systematic Reviews in Pharmacy **11(12)**, 1362-1364 (2020) doi:10.31838/srp.2020.12.201
16. E.S. Sergushina, O.V. Kabanov, V.A. Bogatyrskaya, E3S Web of Conferences **244** (2021) doi:10.1051/e3sconf/202124412027 Retrieved from www.scopus.com
17. S.E. Sergeevna, O.V. Kabanov, V.S. Kolesnik et al, Industrial Engineering and Management Systems **20(2)**, 297-303 (2021) doi:10.7232/iems.2021.20.2.297